



1/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:DERWENT WPI
(c) 2000 Derwent Info Ltd. All rts. reserv.

011885385 **Image available**
WPI Acc No: 1998-302295/199827
XRPX Acc No: N98-236871

Network authentication system for multiple services - notifies address of particular service to partition system after checking received user ID and password with reference to table

Patent Assignee: FUJITSU LTD (FUJIT)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 10105516	A	19980424	JP 97116899	A	19970507	199827 B

Priority Applications (No Type Date): JP 96122914 A 19960517

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
JP 10105516	A	8	G06F-015/00	

Abstract (Basic): JP 10105516 A

The system detects calling to the access point of the network. Then, the user ID and password are forwarded to a network authentication mechanism (6).

The mechanism checks the user ID and password with reference to a table and notifies an address of a particular service to a partition system (4). The partition system is connected to several services.

ADVANTAGE - Raises reliability of network security. Reduces burden of security management.

Dwg.1/5

Title Terms: NETWORK; AUTHENTICITY; SYSTEM; MULTIPLE; SERVICE; NOTIFICATION; ADDRESS; SERVICE; PARTITION; SYSTEM; AFTER; CHECK; RECEIVE; USER; ID; PASSWORD; REFERENCE; TABLE

Derwent Class: T01; W01

International Patent Class (Main): G06F-015/00

International Patent Class (Additional): G06F-001/00; G06F-013/00;

H04L-012/22; H04M-003/42; H04M-011/00

File Segment: EPI

1/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2000 JPO & JAPIO. All rts. reserv.

05822416 **Image available**
NETWORK AUTHENTICATION SYSTEM

PUB. NO.: 10-105516 A]
PUBLISHED: April 24, 1998 (19980424)
INVENTOR(s): SAWA HIROSHI
APPLICANT(s): FUJITSU LTD [000522] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 09-116899 [JP 97116899]
FILED: May 07, 1997 (19970507)
INTL CLASS: [6] G06F-015/00; G06F-001/00; G06F-013/00; H04L-012/22; H04M-003/42; H04M-011/00
JAPIO CLASS: 45.4 (INFORMATION PROCESSING -- Computer Applications); 36.4 (LABOR SAVING DEVICES -- Service Automation); 44.3 (COMMUNICATION -- Telegraphy); 44.4 (COMMUNICATION -- Telephone); 45.2 (INFORMATION PROCESSING -- Memory Units); 45.9 (INFORMATION PROCESSING -- Other)

ABSTRACT

PROBLEM TO BE SOLVED: To improve the reliability of network security and to improve the security management of a service provider or to reduce the burden of security management by performing the security management at the entrance of a network by performing user authentication on the network when providing plural services from the same public access point, and connecting the access point while distributing it to the relevant service.

SOLUTION: A distributing mechanism 4 detects an incoming call from a user terminal 1 through a public line 2 to the access point of a certain network, transfers a user ID and a password to a network authentication mechanism 6 and connected any service designated out of plural services. While referring to a table 9 based on the user ID and the password transferred from this distributing mechanism 4, the relevant user ID and password are checked and in case of OK, the address of the relevant service is reported to the distributing mechanism 4.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-105516

(43) 公開日 平成10年(1998) 4月24日

(51) Int.Cl.⁸

識別記号

F I

G 0 6 F 15/00

3 3 0

G 0 6 F 15/00

3 3 0 B

1/00

3 7 0

1/00

3 7 0 E

13/00

3 5 1

13/00

3 5 1 A

H 0 4 L 12/22

H 0 4 M 3/42

Z

H 0 4 M 3/42

11/00

3 0 2

審査請求 未請求 請求項の数 4 O L (全 8 頁) 最終頁に続く

(21) 出願番号

特願平9-116899

(22) 出願日

平成9年(1997) 5月7日

(31) 優先権主張番号

特願平8-122914

(32) 優先日

平8(1996) 5月17日

(33) 優先権主張国

日本 (J P)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 澤 博史

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

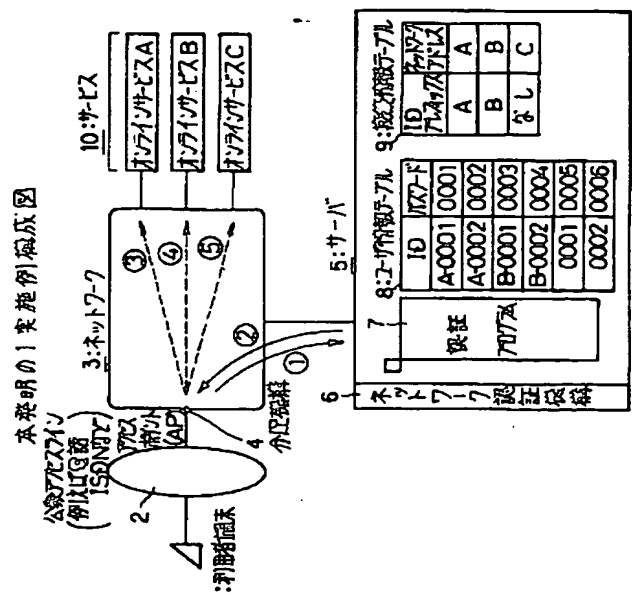
(74) 代理人 弁理士 岡田 守弘

(54) 【発明の名称】 ネットワーク認証システム

(57) 【要約】

【課題】 本発明は、ネットワーク認証システムに関し、同一公衆アクセスポイントから複数のサービスを提供する際に、ネットワークでのユーザ認証を行なうと共に該当するサービスに分配して接続し、ネットワークの入口でセキュリティ管理を行い、ネットワークセキュリティの信頼性を高めると共にサービス提供者のセキュリティ管理を高めたり、セキュリティ管理の負担を軽減したりすることを目的とする。

【解決手段】 利用者端末から公衆回線を介してあるネットワークのアクセスポイントへの着呼を検出して利用者IDおよびパスワードをネットワーク認証機構に転送し、複数のサービスのうちの指定されたサービスに接続する分配機構と、この分配機構から転送されてきた利用者IDおよびパスワードをもとに、テーブルを参照して当該利用者IDおよびパスワードをチェックしてOKのときに該当サービスのアドレスを分配機構に通知するネットワーク認証機構とを備えるように構成する。



【特許請求の範囲】

【請求項1】複数のサービスの認証を行なうネットワーク認証システムにおいて、

利用者端末から公衆回線を介してあるネットワークのアクセスポイントへの着呼を検出して利用者IDおよびパスワードをネットワーク認証機構に転送し、複数のサービスのうちの指定されたサービスに接続する分配機構と、

この分配機構から転送されてきた利用者IDおよびパスワードをもとに、テーブルを参照して当該利用者IDおよびパスワードをチェックしてOKのときに当該サービスのアドレスを上記分配機構に通知するネットワーク認証機構とを備えたことを特徴とするネットワーク認証システム。

【請求項2】複数のサービスの認証を行なうネットワーク認証システムにおいて、

利用者端末から公衆回線を介してあるネットワークのアクセスポイントへの着呼を検出して利用者IDおよびパスワードを認証サーバ中継機構に転送し、複数のサービスのうちの指定されたサービスに接続する分配機構と、上記分配機構から転送されてきた利用者IDおよびパスワードについて、テーブルを参照して当該利用者IDのサービスの認証を担当するサーバに転送してチェックさせ、OKの返答のあったアドレスを上記分配機構に通知する認証サーバ中継機構と、

上記認証サーバ中継機構から転送されてきた利用者IDおよびパスワードをもとに、テーブルを参照して当該利用者IDおよびパスワードをチェックしてOKのときに当該サービスのアドレスを上記認証サーバ中継機構に通知するサーバとを備えたことを特徴とするネットワーク認証システム。

【請求項3】上記利用者IDの一部を上記サービスに対応づけたことを特徴とする請求項1あるいは請求項2記載のネットワーク認証システム。

【請求項4】利用者端末から公衆回線を介してあるネットワークのアクセスポイントへの着呼を検出して利用者IDおよびパスワードをネットワーク認証機構に転送し、複数のサービスのうちの指定されたサービスに接続する分配機構と、

この分配機構から転送されてきた利用者IDおよびパスワードをもとに、テーブルを参照して当該利用者IDおよびパスワードをチェックしてOKのときに当該サービスのアドレスを上記分配機構に通知するネットワーク認証機構とを機能させるプログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数のサービスの認証を行なうネットワーク認証システムに関するものである。

【0002】

【従来の技術】従来、公衆回線を介してネットワークに接続してサービスを提供する場合、サービス毎に専用のアクセスポイント（例えば専用の電話番号）を設け、当該アクセスポイントからネットワークを介して該当オンラインサービスに接続し、当該オンラインサービスで認証（ユーザIDおよびパスワードの認証）を行なう。

【0003】また、商用オンラインサービス事業者が、同一公衆アクセスポイントから複数のサービスを提供する場合、図4に示すように、単にオンラインサービス毎に分配して接続し、接続先のオンラインサービスの入口で認証をそれぞれ個別に行なうようにしていた。

【0004】また、商用オンラインサービス事業者が、同一公衆アクセスポイントから複数のサービスを提供する場合、図5に示すように、あるオンラインサービスで認証を行い、ゲートウェイ機能によって他のオンラインサービスに接続するようにしていた。

【0005】以下図4および図5の構成および動作を簡単に説明する。図4は、従来技術の説明図（その1）を示す。図4において、公衆アクセスラインは、利用者端末からオンラインサービスの提供を受けるためのアクセスポイントAPに接続するための公衆網である。

【0006】ネットワークは、オンラインサービスの提供を行なう事業者のネットワークである。オンラインサービスA、Bは、複数の種類のサービス、例えばパソコン通信、インターネット接続サービスなどのオンラインサービスを提供するサーバなどであって、オンラインサービス機能、およびユーザ認証機能などから構成されるものである。

【0007】オンラインサービス機能は、オンラインで各種サービスを利用者に提供するものである。ユーザ認証機能は、ユーザのユーザIDおよびパスワードの認証を行なうものである。

【0008】次に、動作を説明する。

利用者端末からアクセスポイントに電話する。

で電話を受信したネットワークが利用者端末からの指定をもとに該当するオンラインサービスAあるいはオンラインサービスBに接続する。

【0009】で接続されたオンラインサービスAあるいはオンラインサービスBがユーザIDおよびパスワードの認証を行い、OKのときにサービスの提供をそれぞれ行なう。

【0010】図5は、従来技術の説明図（その2）を示す。図5において、公衆アクセスラインは、利用者端末からオンラインサービスの提供を受けるためのアクセスポイントAPに接続するための公衆網である。

【0011】ネットワークは、オンラインサービスの提供を行なう事業者のネットワークである。オンラインサービスAは、オンラインサービスを提供するサーバなどであって、ここでは、ゲートウェイ機能、オンラインサービス機能、およびユーザ認証機能などから構成される

ものである。

【0012】ゲートウェイ機能は、該当する他のオンラインサービスに転送するものである。オンラインサービス機能は、オンラインで各種サービスを利用者に提供するものである。

【0013】ユーザ認証機能は、ユーザのユーザIDおよびパスワードの認証を行なうものである。次に、動作を説明する。

【0014】 利用者端末からアクセスポイントに電話する。

で電話を受信したネットワークがここでは固定的な1つのオンラインサービスAに接続する。

【0015】 で接続されたオンラインサービスAがユーザIDおよびパスワードの認証を行い、OKのときにサービスを提供、あるいはゲートウェイ機能が更に他のオンラインサービスに接続する。

【0016】 でゲートウェイ機能によって接続された他のオンラインサービス、例えばオンラインサービスBがサービスを提供、あるいは更にユーザIDおよびパスワードの認証を行い、OKのときにサービスの提供を行なう。

【0017】

【発明が解決しようとする課題】 上述したように、従来の図4の構成のもとでは、(1) 異なるオンラインサービスで、アクセスポイントを共用できるが、(2) ネットワーク側でのユーザ認証ができなく(3) オンラインサービスを提供する側でユーザ認証(ユーザIDおよびパスワードによる認証)を行なうため、ネットワークの入口で認証を行なうことができなくセキュリティに欠けると共に、新たなサービスを提供するオンラインサービスでは全ての認証を行ってセキュリティを確保する必要が生じてしまうという問題があった。

【0018】 また、上述したように、従来の図5の構成のもとでは、(1) 異なるオンラインサービスで、アクセスポイントを共用できるが、(2) ネットワーク側でのユーザ認証がなく(3) オンラインサービスを提供する側でユーザ認証(ユーザIDおよびパスワードによる認証)を行なう(4) ゲートウェイ機能を持たないオンラインサービスは、ゲートウェイ機能を有するオンラインサービスのユーザからしかサービス提供を受けることができないため、ネットワークの入口で認証を行なうことができなくセキュリティに欠けると共に、新たなサービスを提供するオンラインサービスでは全ての認証を行ってセキュリティを確保する必要が生じてしまい、更にゲートウェイ機能の有無によって受けられるサービスに制限を生じてしまうという問題があった。

【0019】 本発明は、これらの問題を解決するため、同一公衆アクセスポイントから複数のサービスを提供する際に、ネットワークでのユーザ認証を行なうと共に該当するサービスに分配して接続し、ネットワークの入口

でセキュリティ管理を行い、ネットワークセキュリティの信頼性を高めると共にサービス提供者のセキュリティ管理を高めたり、セキュリティ管理の負担を軽減したりすることを目的としている。

【0020】

【課題を解決するための手段】 図1および図2を参照して課題を解決するための手段を説明する。図1および図2において、利用者端末1は、利用者IDおよびパスワードを入力してサービスを利用するものである。

10 【0021】 分配機構4は、利用者端末1からの着呼を検出して利用者IDおよびパスワードをネットワーク認証機構6や認証サーバ中継機構12に転送したり、複数のサービスのうちの指定されたサービス10に接続したりなどするものである。

【0022】 サービス10は、各種サービスを提供するものである。次に、動作を説明する。ネットワーク3の分配機構4が利用者端末1から公衆回線を介してアクセスポイントへの着呼を検出し、利用者IDおよびパスワードをネットワーク認証機構6に転送し、ネットワーク
20 認証機構6が利用者IDおよびパスワードをもとにテーブルを参照しチェックしてOKのときにサービスのアドレスを分配機構4に通知し、分配機構4が指定されたアドレスに接続し、利用者端末1と該当するサービス10を接続し、当該利用者端末1がサービス10からサービス提供を受けるようにしている。

【0023】 また、ネットワーク3の分配機構4が利用者端末1から公衆回線を介してアクセスポイントへの着呼を検出し、利用者IDおよびパスワードを認証サーバ中継機構12に転送し、認証サーバ中継機構12がテーブルを参照して当該利用者IDのサービスの認証を担当するサーバに転送し、サーバが転送されてきた利用者IDおよびパスワードをもとにテーブルを参照して当該利用者IDおよびパスワードをチェックしてOKのときにサービスのアドレスを認証サーバ中継機構を介して分配機構4に通知し、分配機構4が指定されたアドレスに接続し、利用者端末1と該当するサービス10を接続し、
30 当該利用者端末1がサービス10からサービス提供を受けるようにしている。

【0024】 この際、利用者IDの一部をサービス10に対応づけるようにしている。従って、同一公衆アクセスポイントから複数のサービス提供する際に、ネットワークでのユーザ認証を行なうと共に該当するサービス10に分配して接続し、ネットワークの入口でセキュリティ管理を行うことにより、ネットワークセキュリティの信頼性を高めると共にサービス提供者のセキュリティ管理を高めたり、セキュリティ管理の負担を軽減したりすることが可能となる。

【0025】

【発明の実施の形態】 次に、図1から図3を用いて本発明の実施の形態および動作を順次詳細に説明する。ここ
50

5

で、図1の各機構を機能させるプログラムを図示外の記憶媒体から読み出して該計算機システム（サーバなど）の主記憶上にローディングして起動し、以下に説明する各種処理を実行させるものである。

【0026】図1は、本発明の1実施例構成図を示す。図1において、利用者端末1は、利用者が操作して利用者IDおよびパスワードを入力してサービス10に接続し、各種サービスの提供を受けるためのものである。

【0027】公衆アクセスライン2は、ネットワーク3の任意のアクセスポイントに接続するものであって、例えば公衆回線である電話回線やISDN回線などである。利用者端末1は、この公衆アクセスライン2を用いてアクセスポイントAPの特定の電話番号に発呼し、サービス10と接続して各種サービスの提供を受けるようにしている。

【0028】ネットワーク3は、公衆アクセスラインの特定のアクセスポイントから接続する、サービス提供者側のネットワークであって、ここでは、分配機構4などを有するものである。

【0029】分配機構4は、公衆アクセスラインからネットワーク3のアクセスポイントへの着信を受信したり、利用者端末1から受信した利用者IDおよびパスワードをネットワーク認証機構6に転送したり、ネットワーク認証機構6から通知されたアドレスのサービス10に、着呼した呼を接続したりなどするものである。

【0030】サーバ5は、各種処理を行なうものであって、ここでは、ネットワーク認証機構6などから構成されるものである。ネットワーク認証機構6は、利用者IDおよびパスワードをもとに認証を行なうものであって、ここでは、認証プログラム7、ユーザ情報テーブル8、および接続情報テーブル9などから構成されるものである。

【0031】認証プログラム7は、利用者IDおよびパスワードについて、ユーザ情報テーブル8を参照して認証を行い、OKのときにサービス提供を行なうサービス10のアドレスを接続情報テーブル9から取り出したりなどするものである。

【0032】ユーザ情報テーブル8は、利用者IDおよびパスワードを登録したものである。接続情報テーブル9は、利用者にサービスを提供するサービス10のアドレスを登録したものである。

【0033】次に、動作を説明する。図1において、は、ユーザ認証要求（利用者ID／パスワード認証要求）を行なう。これは、分配機構4が利用者端末1から公衆アクセスライン2によってアクセスポイントAPに着呼したときに、送信されてきた利用者IDおよびパスワードをサーバ5に転送する。

【0034】は、ユーザ認証回答（利用者ID／パスワードチェック回答、および接続ネットワークアドレス回答）を行なう。これは、で転送を受けた利用者ID

6

およびパスワードについて、サーバ5のネットワーク認証機構6を構成する認証プログラム7がユーザ情報テーブル8を参照して認証を行い（利用者IDおよびパスワードが一致するかのチェックを行い）、OKのときに接続情報テーブル9を参照して利用者IDのプレフィックスに対応するネットワークアドレス（プレフィックスによって予め定められているサービス10のアドレス）を取り出し、分配機構4に通知する。

【0035】は、IDプレフィックスがAの場合の接続である。これは、分配機構4がで通知されたネットワークアドレスがAの場合に、アクセスポイントに着呼した呼をネットワークアドレスAのオンラインサービスAに接続する。

【0036】同様に、は、IDプレフィックスがBあるいはCの場合の接続である。これは、分配機構4がで通知されたネットワークアドレスがBあるいはCの場合に、アクセスポイントに着呼した呼をネットワークアドレスBのオンラインサービスBに接続、あるいはネットワークアドレスCのオンラインサービスCに接続する。

【0037】以上によって、利用者端末1から公衆アクセスラインを介してネットワークのアクセスポイントAPに着呼があったときに、送信されてきた利用者IDおよびパスワードをネットワーク認証機構6に転送して認証を行い、OKのときに通知された該当するオンラインサービスに接続し、サービスの提供を行なうことにより、ネットワークの入口で認証を行ってネットワークセキュリティを高信頼性にすることができると共に、ネットワーク認証を行った後に該当するサービス10に振り分けて接続し、当該サービス10で更に認証を行ってセキュリティを高めたり、あるいはネットワークの入口で既に認証がされているので当該サービス10の入口で認証を省略したりすることが可能となる。

【0038】図2は、本発明の他の実施例構成図を示す。ここで、利用者端末1、公衆アクセスライン2、ネットワーク3、およびサービス10は、図1の同一番号のもので同じであるので説明を省略する。

【0039】図2において、サーバ11は、各種処理を行なうものであって、ここでは、認証サーバ中継機構12などから構成されるものである。認証サーバ中継機構12は、ネットワーク3の分配機構4から転送されてきた利用者IDおよびパスワードを該当するネットワーク認証機構16に転送したり、ネットワーク認証機構16から通知された接続先のネットワークアドレスを分配機構4に通知したりなどするものであって、認証サーバ選択／中継プログラム13およびサーバ対応テーブル14などから構成されるものである。

【0040】認証サーバ選択／中継プログラム13は、サーバ対応テーブル14を参照して利用者IDのプレフィックスをもとに認証サーバを取り出し、利用者IDお

10

20

30

40

50

7

よびパスワードをこのサーバに転送したり、認証結果を受け取ったときに分配機構4に通知したりなどするものである。

【0041】サーバ対応テーブル14は、利用者IDのプレフィックスに対応づけて認証を行なう認証サーバを予め登録したものである。サーバ15は、利用者IDおよびパスワードをもとに認証を行なうものであって、ここでは、ネットワーク認証機構16などから構成されるものである。

【0042】ネットワーク認証機構16は、利用者IDおよびパスワードをもとに認証を行なうものであって、ここでは、認証プログラム17、ユーザ情報テーブル18、およびアドレステーブル19などから構成されるものである。このようにネットワーク認証機構16をサービス10毎に設けたことにより、サービス10毎に一元的に利用者IDおよびパスワードを管理し、図2に示す本願発明のネットワーク3の入口で認証を行なうルートと、図2以外の従来のサービス10毎の専用のアクセスポイントへの利用者端末1からの利用者IDおよびパスワードによる認証を並行して行なう場合に、サービス毎に一元的に利用者IDおよびパスワードを容易に管理（利用者IDおよびパスワードの新規登録、修正、削除など）することが可能となる。

【0043】認証プログラム17は、利用者IDおよびパスワードについて、ユーザ情報テーブル18を参照して認証を行い、OKのときにサービス提供を行なうサービス10のアドレスをアドレステーブル19から取り出したりなどするものである。

【0044】ユーザ情報テーブル18は、利用者IDおよびパスワードを登録したものである。アドレステーブル19は、利用者にサービスを提供するサービス10の接続ネットワークアドレスを登録したものである。

【0045】次に、動作を説明する。図2において、は、ユーザ認証要求（利用者ID／パスワード認証要求）を行なう。これは、分配機構4が利用者端末1から公衆アクセスライン2によってアクセスポイントAPに着呼したときに、送信されてきた利用者IDおよびパスワードをサーバ11転送する。

【0046】は、IDプレフィックスにより認証サーバを選択し、ユーザ認証要求を中継する。これは、で転送を受けた利用者IDおよびパスワードについて、サーバ11の認証サーバ中継機構12を構成する認証サーバ選択／中継プログラム13がサーバ対応テーブル14を参照して利用者IDのプレフィックスと一致する認証サーバを取り出し、ユーザ認証要求（利用者ID／パスワード認証要求）を中継する。

【0047】は、ユーザ認証回答（利用者ID／パスワードチェックおよび接続ネットワークアドレス回答）を行なう。これは、で中継を受けた利用者IDおよびパスワードについて、サーバ15のネットワーク認証機

8

構16を構成する認証プログラム17がユーザ情報テーブル18を参照して認証を行い（利用者IDおよびパスワードが一致するかのチェックを行い）、OKのときにアドレステーブル19を参照して接続ネットワークアドレスを取り出し、認証サーバ中継機構12に通知する。

【0048】は、各サーバからのユーザ認証回答をアクセスポイントの分配機構4に中継する。これは、で各サーバからのユーザ認証回答（OKのときの接続ネットワークアドレスの回答）を分配機構4に通知する。

【0049】は、IDプレフィックスがAAAの場合の接続である。これは、分配機構4がで通知された接続ネットワークアドレスがA. A. A. の場合に、アクセスポイントに着呼した呼をネットワークアドレスA. A. A. のオンラインサービスAに接続する。

【0050】同様に、は、IDプレフィックスがBBBあるいはCCCの場合の接続である。これは、分配機構4がで通知された接続ネットワークアドレスがB. B. B. B. あるいは接続ネットワークアドレスがC. C. C. C. の場合に、アクセスポイントに着呼した呼をネットワークアドレスB. B. B. B. のオンラインサービスBに接続、あるいはネットワークアドレスC. C. C. C. のオンラインサービスCに接続する。

【0051】以上によって、利用者端末1から公衆アクセスラインを介してネットワークのアクセスポイントAPに着呼があったときに、送信されてきた利用者IDおよびパスワードを認証サーバ中継機構12に転送し、該当するネットワーク認証機構16に中継して認証を行い、OKのときに通知された該当するオンラインサービスに接続し、サービスの提供を行なうことにより、ネットワークの入口で認証を行ってネットワークセキュリティを高信頼性にすることができると共に、ネットワーク認証を行った後に該当するサービス10に振り分けて接続し、当該サービス10で更に認証を行ってセキュリティを高めたり、あるいはネットワークの入口で既に認証がされているので当該サービス10の入口で認証を省略したりすることが可能となると共に、更に、サービス10毎にネットワーク認証機構16を設けて利用者IDおよびパスワードの認証を行なうことにより、サービス10毎に一元的に管理（利用者IDおよびパスワードの新規登録、修正、削除など）を行なうことが可能となる。

【0052】次に、図3を用いて図2の構成の動作を詳細に説明する。図3は、本発明の動作説明図を示す。ここで、サーバSは図2のサーバ11を表し、サーバSAA、サーバSBBB、サーバSCCCは図2のサーバ15を表し、アクセスポイントは図2のアクセスポイントを表す。

【0053】図3において、S1は、ID／PWを受信する。これは、図2のサーバ11の認証サーバ中継機構12が利用者端末1からの利用者IDおよびパスワードを受信する。

【0054】S2は、先頭3文字を識別し、該当サーバにID/PWを渡す。これは、S1で受信した利用者IDの先頭3文字を識別、例えば利用者IDのプレフィックスである先頭の3文字“AAA”を識別し、図2のサーバ対応テーブル14を参照して認証サーバ“SAAA”を取り出し、この認証サーバ“SAAA”に利用者IDおよびパスワードを渡す。そして、この例では、S3ないしS9を行なう。

【0055】S3は、オンラインサービスA用認証を行なう（IDデータに対応する認証チェック）。これは、S2で利用者IDプレフィックス=AAAと判明し、利用者IDおよびパスワードをサーバSAAAが渡されたので、図2の認証プログラム17がユーザ情報テーブル18を参照し、利用者IDおよびパスワードが登録されているかチェックする。OKの場合には、S4でネットワークアドレス（図2のアドレステーブル19から取り出した接続ネットワークアドレス）をアクセスポイント（分配機構4）に返し、S6でオンラインサービスAに呼を接続し、利用者端末1がオンラインサービスAと接続してサービス提供を受ける。一方、NGの場合には、S7で不可通知を返し、S8で受信した不可通知をアクセスポイントに返し、S9で分配機構4が呼を切断する。

【0056】同様に、S2で利用者IDプレフィックス=BBBあるいは利用者IDプレフィックス=CCCと判明した場合、S13ないしS19、あるいはS23ないしS29によって認証OKのときにオンラインサービスBあるいはオンラインサービスCに接続したり、一方、認証NGのときに切断したりする。

【0057】

【発明の効果】以上説明したように、本発明によれば、同一公衆アクセスポイントから複数のサービス提供する際に、ネットワークでのユーザ認証を行なうと共に該当するサービス10に分配して接続し、ネットワークの入口でセキュリティ管理を行う構成を採用しているため、ネットワークセキュリティの信頼性を高めると共にサービス提供者のセキュリティ管理を高めたり、セキュリティ管理の負担を軽減したりすることができる。

【図面の簡単な説明】

【図1】本発明の1実施例構成図である。

【図2】本発明の他の実施例構成図である。

【図3】本発明の動作説明図である。

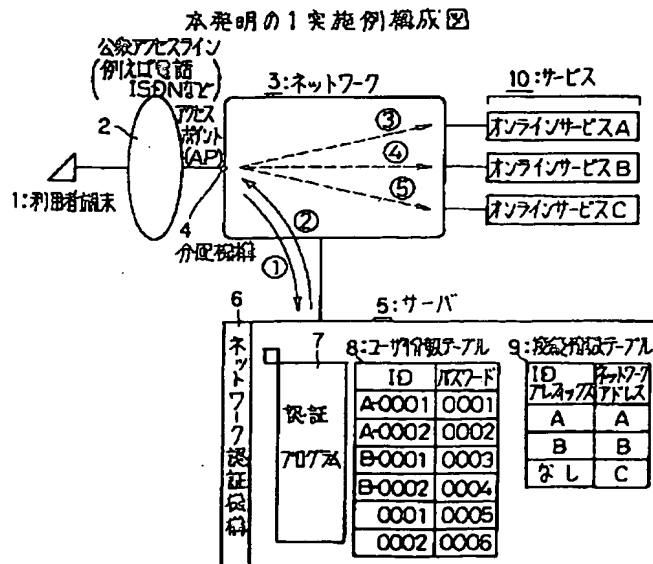
【図4】従来技術の説明図（その1）である。

【図5】従来技術の説明図（その2）である。

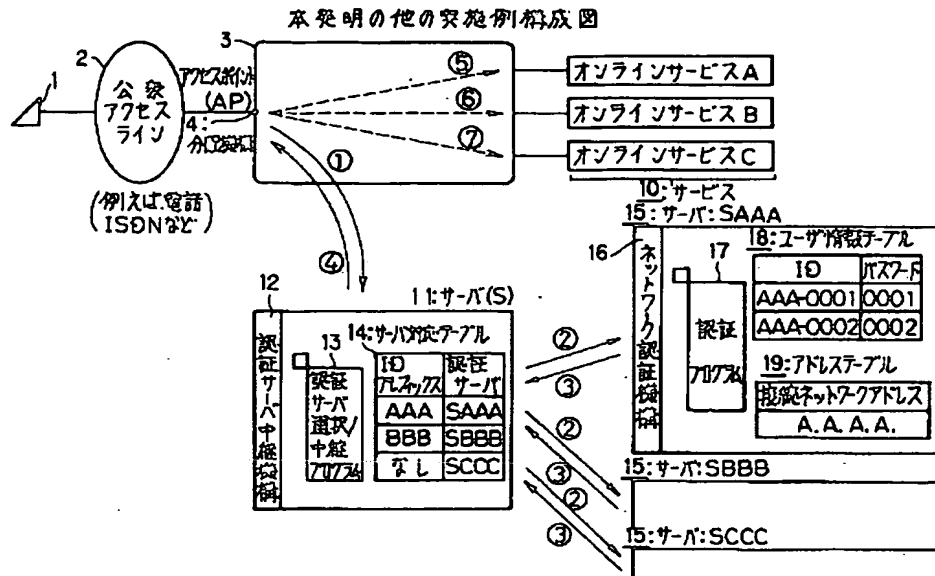
【符号の説明】

- 1：利用者端末
- 2：公衆アクセスライン（公衆回線網）
- 3：ネットワーク
- 4：分配機構
- 5、11、15：サーバ
- 6、16：ネットワーク認証機構
- 7、17：認証プログラム
- 8、18：ユーザ情報テーブル
- 9：接続情報テーブル
- 10：サービス
- 12：認証サーバ中継機構
- 13：認証サーバ選択／中継プログラム
- 14：サーバ対応テーブル
- 19：アドレステーブル

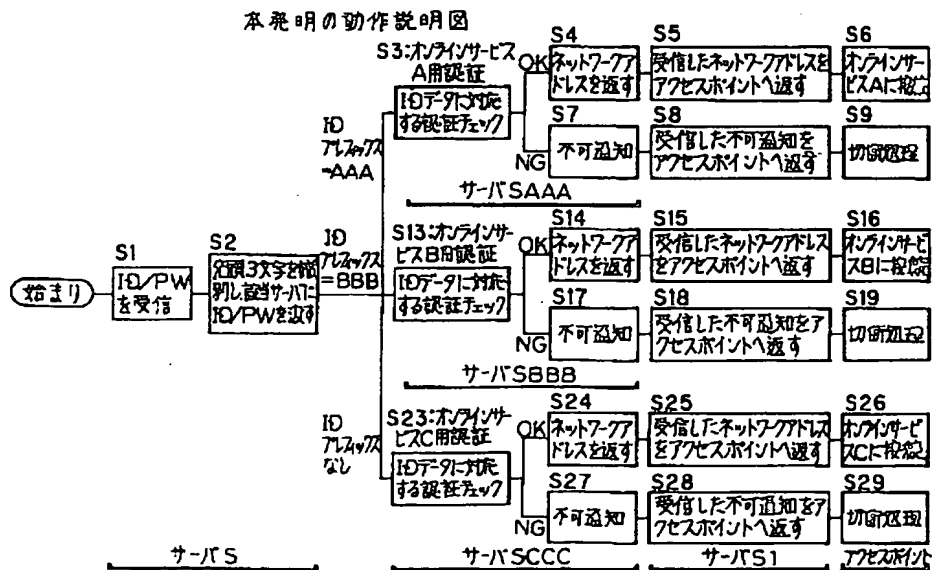
【図1】



【図2】

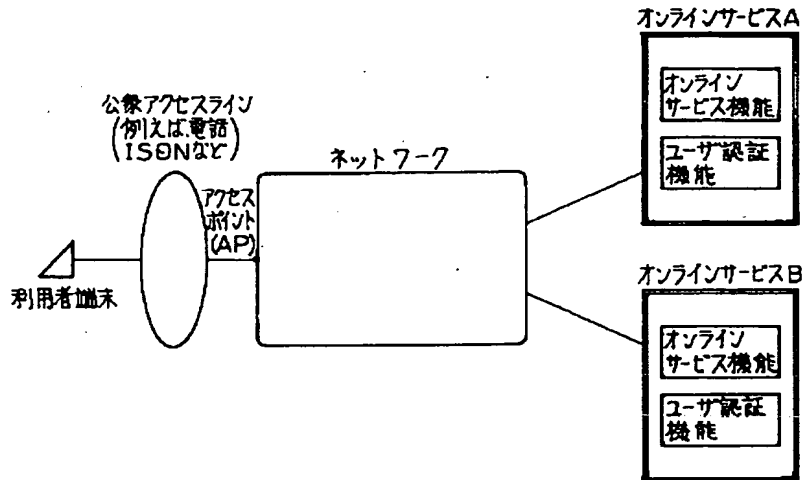


【図3】



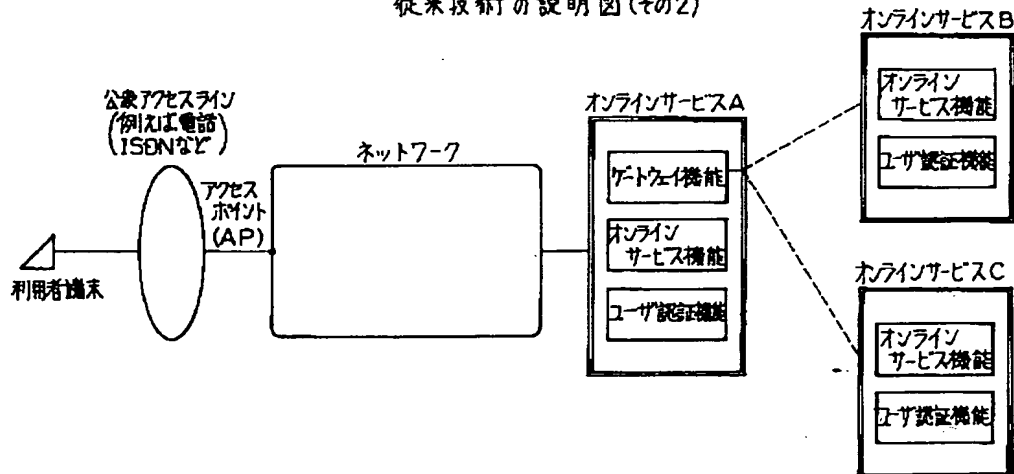
【図4】

従来技術の説明図(その1)



【図5】

従来技術の説明図(その2)



フロントページの続き

(51) Int. Cl.⁶
H04M 11/00識別記号
302FI
H04L 11/26